REMARKS

In the Claims

Claims 1-13 are pending in the application and stand rejected under 35 USC § 103 based on various cited references, including U.S. Patent No. 5,757,912 to Blow ("Blow") and U.S. Patent Application Publication No. 2003/0112970 to Mitra ("Mitra").

An obvious rejection under 35 USC §103(a) requires that the combination of cited references yield all of the claim limitations. Also, the claim must be **read as a whole** to avoid the impermissible assembling bits and pieces of prior art to reconstruct Applicant's claimed invention using hindsight.

For the reasons outlined below, Applicants respectfully traverse the rejections of claims 1-13.

Claims 1-4 and 9

Independent claims 1 and 9 stand rejected under 35 USC § 103 based on Blow in view of Mitra.

In the rejection of claims 1 and 9, the Examiner correctly points out that Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits.

The Examiner then asserts on page 4, item 13 of the Office Action, that "Mitra discloses encrypting key bits (paragraph 0013) and transmitted [sic: transmitting] the encrypted key bits (paragraphs 0013, 0014, i.e., transmitting either classically or quantum)."

By way of review, Mitra discloses "methods of generating unbreakable identical keys at two or more distant stations." Paragraph [0001]. A closer review of Mitra, however, indicates that Mitra involves performing operations on **keys that already exist at Alice and Bob**, e.g., by forming a number of "encrypted double keys" based on an already shared key. See, e.g., paragraph [0013]. The reference in paragraph [0014] that the cryptographic system can be classic or quantum seems

2

to be directed to the point that either type of system can be used to generate the keys that are ultimately shared by Alice and Bob, and that Mitra envisions Alice and Bob to be able to encrypt and decrypt such keys using the techniques set forth in Mitra.

It is important to note that Mitra *starts* from the point where Alice and Bob *already share a secret key* (see, e.g., paragraph [0011]). In contrast, Applicants' claimed invention is directed to "performing quantum key distribution," which means it is ultimately directed to *establishing* a quantum key between Alice and Bob. That is to say, prior to carrying out Applicants' claimed invention, *Alice and Bob have yet to share a key.* Thus, the *Mitra invention starts where Applicant's invention ends,* and there is *no overlap between the two inventions.*

In Applicant's invention, there is no encryption of the "key" as this term is used in Mitra. There is some unfortunate but understandable confusion on this point because the Applicants and Mitra use the same phrase "key bit" to describe *two different things.* Applicants use the term "key bit" to describe one of the two types of bits (the other being the "basis bit") used to *encode an optical pulse* to form a *qubit.* Note that neither a "qubit" nor a "key bit" in Applicants' invention is actually part of a key used to encrypt information. A qubit is simply an encoded optical pulse that needs to be processed according to QKD protocols before a "quantum key" can be formed. In contrast, a "key bit" as this term is used by Mitra is one bit of a key that is used to encrypt information, which key is assumed to already be shared by Bob and Alice. In Applicants invention, this would be called, for example, a "quantum-key bit."

Because Mitra is only concerned with *encrypting existing keys to form new keys,* it does not disclose any of the claim limitations of Applicants' claimed invention, which is directed to encrypting qubits using a QKD system.

In view of the above, the combination of Blow and Mitra cannot yield all of the limitations in Applicant's claim 1. Consequently, a *prima facie* case for obviousness cannot be established using these references.

The obviousness rejection of Applicant's claims 1 and 9 is therefore traversed

3

and withdrawal of the rejection is earnestly requested. For the same reasons, the obviousness rejection as applied to claims 2-4 depending from claim 1 is also traversed, and withdrawal of the obviousness rejection of these dependent claims is earnestly requested.

Claims 5-7

Claim 5 is rejected for essentially the same reasons as claims 1 and 9, and further in view of the article "Applied Cryptography" by Schneier ("Schneier").

The Schneier reference is directed to classical encryption, and Applicant's invention admits to using classical encryption since it is invention is entitled "QKD with classical bit encryption." However, it is the **combination of claim elements taken as a whole** that combine classical encryption with quantum cryptography in **a unique and non-obvious way** to provide enhanced security over existing quantum encryption systems. The Schneier reference does not fill in any of the gaps left by Blow and Mitra in attempting to arrive at Applicants' claimed invention.

Accordingly, the rejection of claim 5 and its dependent claims 6 and 7 is traversed for the same reasons set forth above in connection with the obviousness rejection of claims 1 and 9, and withdrawal of the obviousness rejection of these claims is earnestly requested.

Claim 8-13

Claims 8-13 are rejected under 35 USC §103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend ("Townsend") in view of U.S. Patent Application Publication No. 2006/0120529 to Gisen et al. ("Gisen"), and further in view of Schneier and Mitra

Applicant reiterates here that a closer reading of Mitra reveals that *Mitra does not address forming encrypted qubits in the manner claimed by Applicant and instead is directed at encrypting existing keys already shared by Alice and Bob to form new keys.*

As stated above, the Schneier reference is directed to classical encryption,

and Applicant's invention admits to using classical encryption since it is invention is entitled "QKD with classical bit encryption." However, it is the **combination of claim elements taken as a whole** that combine classical encryption with quantum cryptography in **a unique and non-obvious way** to provide enhanced security over existing quantum encryption systems.

There is absolutely no teaching, suggestion or motivation in any of the cited references to form encrypted qubits using encrypted key bits in the manner claimed by the Applicant. Moreover, **the combination of the cited references cannot yield all of the limitations in Applicant's claims 8-13.** Consequently, a *prima facie* case for obviousness cannot be established using the cited references.

Accordingly, the obviousness rejection of Applicant's claims 8-13 is traversed and withdrawal of the rejection is earnestly requested.

CONCLUSION

Applicants respectfully submit that the obviousness rejections of claims 1-13 are traversed because the cited references do not yield Applicant's claimed invention and so cannot reasonably be said to establish a *prima facie* case for obviousness. Applicants' therefor respectfully submit claims 1-13 as presently presented are in condition for allowance and earnestly request a Notice of Allowance be issued in due course.

The Examiner is encouraged to contact the undersigned Attorney at 941-378-2744 to discuss any questions that may arise in connection with this Amendment.

Respectfully Submitted,

By: _____ Date: February 23, 2009
Joseph E. Gortych
Reg. No. 41,791

Customer No. **53590**

Opticus IP Law PLLC
7791 Alister Mackenzie Dr
Sarasota, FL 34240 USA

Phone: 941-378-2744
Fax: 321-256-5100
E-mail: jg@opticus-ip.com

6